



TITLE:

Buratti-Del Fra型の高次元双対超卵形 (代数的組合せ論および関連する群と代数)

AUTHOR(S):

谷口, 浩朗

CITATION:

谷口, 浩朗. Buratti-Del Fra型の高次元双対超卵形 (代数的組合せ論および関連する群と代数). 数理解析研究所講究録 2010, 1687: 77-83

ISSUE DATE:

2010-05

URL:

<http://hdl.handle.net/2433/141490>

RIGHT:

Buratti-Del Fra 型の高次元双対超卵形

香川高専 谷口浩朗 (Hiroaki Taniguchi)*
Kagawa National College of Technology

1 はじめに

射影空間 $PG(m, 2)$ 内の高次元双対超卵形 (dimensional dual hyperoval, DHO) は C. Huybrechts と A. Pasini [6] により以下のように定義された.

定義 1 ($GF(q)$ 上の DHO). m -次元射影空間 $PG(m, q)$ における d -次元部分空間の集合 S が, $PG(m, q)$ における d -次元双対超卵形であるとは, 以下のことが成り立つことである:

- (1) S に属するどの 2 個の d -部分空間も 1 点で交わり,
- (2) S に属するどの異なる 3 個の d -部分空間も共通点を持たず,
- (3) S に属する d -部分空間達は $PG(m, q)$ を生成し,
- (4) S は $q^d + q^{d-1} + \cdots + q + 2$ 個の d -部分空間から成る.

本稿では $GF(2)$ 上の高次元双対超卵形のみを考察するが, $q > 2$ の場合の双対超卵形も同様に研究されている. 有名なものとしては, M_{22} が作用する $PG(5, 4)$ における 2 次元双対超卵形の例がある. (たとえば [7] 参照.) $GF(2)$ 上の d -次元の双対超卵形が生成する射影空間の次元 n については, $2d \leq n \leq d(d+3)/2 + 2$ が示されている [14] が, 本当は $2d \leq n \leq d(d+3)/2$ であろうと予想されている. その最大の次元と考えられる $PG(d(d+3)/2, 2)$ には, 現在

- (1) Huybrechts' DHO [5],
 - (2) Buratti-Del Fra's DHO [1],[3],
 - (3) Veronesean DHO [11], [14],
 - (4) Veronesean DHO の変形 [9],
- の 4 種類の (同型でない) 双対超卵形が構成されている.

*E-mail address: taniguchi@dg.kagawa-nct.ac.jp

さて、吉荒は (1) の Huybrechts' DHO の quotient である高次元双対超卵形 (DHO) を、Quadratic な APN 関数を用いて構成した. (quotient または cover の定義については A. Psini [8], 8.2 および 8.3 をご覧下さい.) 本稿では (2) の Buratti-Del Fra's DHO の quotient である高次元双対超卵形 (DHO) を、Quadratic な APN 関数を用いて構成することを考える.

定義 2 (APN 関数). $GF(2)$ 上のベクトル空間 H から W への写像 f が APN (almost perfect nonlinear) であるとは、 H の (すべての) 0 と異なる元 a および W の (すべての) 元 b に対し $|\{x \in H \mid f(x+a) + f(x) = b\}| \leq 2$ が成り立つこととする.

APN 関数は、DES 暗号の S-Box の設計との関係で研究されており、近年 (2005 年頃から) 非常に研究が進展している. (APN function, Cryptography で検索すると多くの論文が出てくる.)

定義 3 (Quadratic な関数). $GF(2)$ 上のベクトル空間 H から W への写像 f は、 $B_f(x, y) := f(x+y) + f(x) + f(y) + f(0)$ が双一次形式であるとき、Quadratic であるという.

Quadratic な APN 関数 f から構成される高次元双対超卵形 S_f は次のように定義される. ([12], [13] 参照.)

例 (吉荒による APN DHO S_f). H を $d+1$ 次元ベクトル空間とし、 $R = \langle B_f(x, y) \mid x, y \in H \rangle$ とする. このとき、 $s \in H$ に対して

$$X(s) := \{(x, B_f(x, s)) \mid x \in H \setminus \{s\}\} \subset PG(H \oplus R)$$

は d -次元部分空間であり $S_f = \{X(s) \mid s \in H\}$ は $PG(H \oplus R)$ における d -次元双対超卵形となる.

この S_f は、Huybrechts' DHO の quotient であることが分かっている.

本稿では $d \geq 4$ の場合、 $GF(2^d)$ 上の Quadratic な APN 関数 f から、Buratti-Del Fra's DHO の quotient である高次元双対超卵形 D_f を $3d$ -次元射影空間 $PG(3d, 2)$ 内に構成する方法を説明する. さらに次の定理の証明を説明する.

定理 1. $d \geq 4$ とし、 f と g を $GF(2^d)$ 上の Quadratic な APN 関数とする. もし d -次元双対超卵形 D_f と D_g が同型であるならば、 f と g は拡大アファイン同値である.

なお、本稿中には、十分詳しい証明を与えることが出来ない場合があります、もし十分詳しい証明が必要な場合にはご連絡を下さい.

定義 4. f と g が拡大アファイン同値であるとは、アフィン同型写像 A_1 , A_2 とアファイン写像 A が存在して $f = A_1 \circ g \circ A_2 + A$ と表せることである.

2 Buratti-Del Fra 型の双対超卵形の構成

H を $d+1$ 次元ベクトル空間とし, $R = \langle B_f(x, y) \mid x, y \in H \rangle$ とする. 以下のことが簡単に分かる.

命題 1. $s, t \in H$ に対して $b(s, t) \in H \oplus R$ を次を満たすように定める.

- (b1) $b(s, s) = (0, 0)$,
- (b2) $b(s, t) = b(t, s)$,
- (b3) $b(s, t) \neq (0, 0)$ if $s \neq t$,
- (b4) $b(s, t) = b(s', t')$ if and only if $\{s, t\} = \{s', t'\}$ in case $s \neq t$ or $s' \neq t'$,
- (b5) $\{b(s, t) \mid t \in H\}$ is a vector space over $GF(2)$, and
- (b6) $\{b(s, t) \mid s, t \in H\}$ generate $H \oplus R$.

このとき, $X(s) := \{b(s, t) \mid t \in H \setminus \{s\}\} \subset PG(H \oplus R)$ は d -次元部分空間であり $S = \{X(s) \mid s \in H\}$ は $PG(H \oplus R)$ における d -次元双対超卵形となる.

定義 5. $\{e_0, e_1, e_2, \dots, e_d\}$ を H の基底とする. $x = e_{i_1} + \dots + e_{i_l}$ に対して $Supp(x) := \{e_{i_1}, \dots, e_{i_l}\} \subset \{e_0, e_1, e_2, \dots, e_d\}$ とし, また $Supp(0) := \emptyset$ と定める. さらに $J(x)$ を次のように定める.

$$\begin{cases} |Supp(x)| \text{ が奇数の場合, } J(x) := Supp(x) \\ |Supp(x)| \text{ が偶数の場合, } J(x) := \{0\} \cup Supp(x) \end{cases}.$$

V を $\{e_1, e_2, \dots, e_d\}$ で生成された H の部分ベクトル空間とし,

$$H \ni x = \sum_{i=0}^d \alpha_i e_i \mapsto \bar{x} = \sum_{i=1}^d \alpha_i e_i \in V$$

とする. ($i = 0, \dots, d$ に対し $\alpha_i \in GF(2)$ である.) ξ を V 上定義された $V \setminus \{0\}$ の特性関数とし, $s, t \in H$ に対して

$$x_{s,t} := \xi(\bar{s} + \bar{t}) + \sum_{w \in J(\bar{t})} \xi(\bar{s} + w) \in GF(2)$$

と定める.

これで, Buratti-Del Fra 型 高次元双対超卵形 D_f が以下のように定義できる.

例 (Buratti-Del Fra 型 DHO D_f). f を H 上の *Quadratic* な APN 関数とする. $H \oplus R$ において $b(s, t)$ を次のように定義する:

$$\begin{aligned} b(s, t) &:= (s + t, B_f(s, t)) \\ &+ x_{\bar{s}, \bar{t}} \sum_{w \in J(\bar{s})} (e_0, B_f(e_0, w)) + \sum_{w \in J(\bar{t})} x_{w, \bar{s}} (e_0, B_f(e_0, w)). \end{aligned} \quad (1)$$

このとき $b(s, t)$ は条件 (b1), (b2), (b5), (b6) を満たす. さらに, 次の和公式も満たすことが確かめられる.

$$b(s, t_1) + b(s, t_2) = b(s, s + t_1 + t_2 + \alpha\{s, t_1, t_2\}e_0),$$

ただし $\alpha\{s, t_1, t_2\} := \xi(\bar{s} + \bar{t}_1) + \xi(\bar{s} + \bar{t}_2) + \xi(\bar{t}_1 + \bar{t}_2) \in GF(2)$ とする.

l を十分大な整数とし, $e_0 \in GF(2^{dl})$ を, $GF(2^d)$ 上 e_0 が $GF(2^{dl})$ を体として生成するように選んでおく. $GF(2^d)$ の基底 $\{e_1, e_2, \dots, e_d\}$ も固定しておく. $GF(2^{dl}) \oplus GF(2^{dl})$ 内でベクトル空間 U を次のように定義する.

$$U := \{(s + t, B_f(s, t)) \mid s, t \in GF(2^d)\}.$$

同様ベクトル空間 W も次のように定義する:

$$W := \langle (e_0, 0), (e_0, B_f(e_0, e_1)), (e_0, B_f(e_0, e_2)), \dots, (e_0, B_f(e_0, e_d)) \rangle.$$

このとき $U = GF(2^d) \oplus GF(2^d)$ であり, $s, t \in GF(2^d)$ のとき, $b(s, t) := (s + t, B_f(s, t))$ 達は $PG(U)$ における吉荒による APN DHO S_f を生成することに注意する. さらに, e_0 の取り方により $(e_0, 0), (e_0, B_f(e_0, e_1)), (e_0, B_f(e_0, e_2)), \dots, (e_0, B_f(e_0, e_d))$ は, 一次独立であるので, W は $(d + 1)$ -次元ベクトル空間である.

補題 1. $H := \langle GF(2^d), e_0 \rangle \subset GF(2^{dl})$ とする. このとき以下が成り立つ.

(1) $U \cap W = \{(0, 0)\}$,

(2) $H \oplus R = U \oplus W$,

(3) f は H 上の *Quadratic* APN 関数と見なせる.

たとえば, 以下のことから $b(s + e_0, t) \in U \oplus W$ がわかる.

$$\begin{aligned} b(s + e_0, t) &= (s + t, B_f(s, t)) + (e_0, B_f(e_0, t)) \\ &+ x_{\bar{s}, \bar{t}} \sum_{w \in J(\bar{s})} (e_0, B_f(e_0, w)) + \sum_{w \in J(\bar{t})} x_{w, \bar{s}} (e_0, B_f(e_0, w)) \\ &= (s + t, B_f(s, t)) + \sum_{w \in J(\bar{t})} (e_0, B_f(e_0, w)) \\ &+ x_{\bar{s}, \bar{t}} \sum_{w \in J(\bar{s})} (e_0, B_f(e_0, w)) + \sum_{w \in J(\bar{t})} x_{w, \bar{s}} (e_0, B_f(e_0, w)). \end{aligned}$$

同様 $b(s, t) \in U \oplus W$, $b(s, t + e_0) \in U \oplus W$, $b(s + e_0, t + e_0) \in U \oplus W$ が成り立つので, $s, t \in H$ に対して $b(s, t)$ 達が生成する空間 $H \oplus R$ が $U \oplus W$ と等しいことが分かる. 次に, 射影 $\pi : U \oplus W \rightarrow U$ の像について考察する. $s, t \in GF(2^d)$ に対して $\bar{b}(s, t) := (s + t, B_f(s, t))$ と定めると, $s, t \in H$ に対して $\pi(b(s, t)) = \bar{b}(\bar{s}, \bar{t})$ となるので以下のことが分かる.

$$\pi : U \oplus W \ni b(s, t) \mapsto \bar{b}(\bar{s}, \bar{t}) \in U.$$

$s \in GF(2^d)$ に対して $\bar{X}_f(s) := \{\bar{b}(s, t) \mid t \in GF(2^d) \setminus \{s\}\} \subset U \setminus \{(0, 0)\}$ とし, \bar{S}_f を以下のように定める.

$$\bar{S}_f := \{\bar{X}_f(s) \mid s \in GF(2^d)\}.$$

\bar{S}_f は吉荒による (APN 関数 f を用いた) $(d-1)$ -次元 APN DHO である. \bar{S}_f が双対超卵形であることを利用して, (つまり (b3) および (b4) は \bar{S}_f については成立しているので) Buratti-Del Fra 型の DHO D_f についても (b3) および (b4) が成り立つことが証明できる. その結果, $PG(U \oplus W) = PG(3d, 2)$ の中に d -次元 Buratti-Del Fra 型の DHO D_f が構成出来ることが分かった. なお, D_f は吉荒による DHO S_f とは (和公式が異なるので) 同型ではない.

3 Buratti-Del Fra 型の DHO の同型問題について

f および g を $GF(2^d)$ 上の Quadratic APN 関数とする. f, g に対して e_0 および e'_0 , $GF(2^d)$ の基底を e_1, \dots, e_d および e'_1, \dots, e'_d と定める. $H := \langle GF(2^d), e_0 \rangle$ および $H' := \langle GF(2^d), e'_0 \rangle$ とする. また

$$\begin{aligned} W_f &:= \langle (e_0, 0), (e_0, B_f(e_0, e_1)), (e_0, B_f(e_0, e_2)), \dots, (e_0, B_f(e_0, e_d)) \rangle, \\ W_g &:= \langle (e'_0, 0), (e'_0, B_g(e'_0, e'_1)), (e'_0, B_g(e'_0, e'_2)), \dots, (e'_0, B_g(e'_0, e'_d)) \rangle. \end{aligned}$$

D_f を $PG(U \oplus W_f)$ における Buratti-Del Fra 型 DHO, D_g を $PG(U \oplus W_g)$ における Buratti-Del Fra 型 DHO とする. また, $X_f(t) := \{b_f(s, t) \mid t \in H\}$, $X_g(t) := \{b_g(s, t) \mid t \in H'\}$ とする. さて, $\Phi : PG(U \oplus W_f) \rightarrow PG(U \oplus W_g)$ により $D_f = \{X_f(t) \mid t \in H\}$ から $D_g = \{X_g(t) \mid t \in H'\}$ への同型写像が導かれると仮定する. このとき, 1対1写像 $\rho : H \rightarrow H'$ があつて $\Phi(X_f(t)) = X_g(\rho(t))$ と表せる. ここで, 高次元双対超卵形の性質より, $s, t_1, t_2 \in H$ に対して以下が成り立つことが分かる.

$$\begin{aligned} \rho(s + t_1 + t_2 + \alpha\{s, t_1, t_2\}e_0) \\ = \rho(s) + \rho(t_1) + \rho(t_2) + \alpha\{\rho(s), \rho(t_1), \rho(t_2)\}e'_0. \end{aligned}$$

そうすると, ρ は線形写像 $A: H \rightarrow H'$ で $A(e_0) = e'_0$ を満たすものを用いて, $\rho(x) = A(x) + h$ と表せることが証明できる. ([3] の Proposition 10 参照.) そうすると

$$\begin{aligned}
& \Phi((e_0, B_f(e_0, w))) \\
&= \Phi(b_f(0, w)) + \Phi(b_f(e_0, w)) \\
&= b_g(\rho(0), \rho(w)) + b_g(\rho(e_0), \rho(w)) \\
&= b_g(h, A(w) + h) + b_g(e'_0 + h, A(w) + h) \\
&= (h + (A(w) + h), B_g(h, A(w) + h)) + \cdots \\
&+ ((e'_0 + h) + (A(w) + h), B_g(e'_0 + h, A(w) + h)) + \cdots \\
&= (e'_0, B_g(e'_0, A(w) + h)) + \cdots \\
&= \sum_{w \in J(\overline{A(w)+h})} (e'_0, B_g(e'_0, w)) + \cdots .
\end{aligned}$$

より $\Phi(W_f) \subset W_g$ が分かる. よって次の写像が導かれる.

$$\bar{\Phi}: U \cong (U \oplus W_f)/W_f \rightarrow (U \oplus W_g)/W_g \cong U.$$

この写像 $\bar{\Phi}$ により, $PG(U)$ における, 吉荒による APN DHO 達 \bar{S}_f と \bar{S}_g の同型が導かれる. さらに, \bar{S}_f が \bar{S}_g と同型ということより, f と g が拡大アフィン同値ということが分かる. ([4] の Theorem 1 を見よ.) 以上のことから, 次の定理が証明された.

定理 1 $d \geq 4$ とし, f と g を $GF(2^d)$ 上の Quadratic な APN 関数とする. もし d -次元双対超卵形 D_f と D_g が同型であるならば, f と g は拡大アフィン同値である.

References

- [1] M. Buratti and A. Del Fra, Semi-Boolean quadruple systems and dimensional dual hyperovals, *Advances in Geometry*. 3 (2003), 245–253.
- [2] A. Del Fra, On d -Dimensional Dual Hyperovals, *Geometriae Dedicata*. 79 (2000), 157–178.
- [3] A. Del Fra and S. Yoshiara, Dimensional dual hyperovals associated with Steiner systems, *European Journal of Combinatorics*. 26 (2005), 173–194.

- [4] E. Edel, On quadratic APN functions and dimensional dual hyperovals, Designs, Codes and Cryptography. 2009
- [5] C. Huybrechts, Dimensional dual hyperovals in projective spaces and $c.AC^*$ geometries, Discrete Mathematics. 255 (2002), 503–532.
- [6] C. Huybrechts and A. Pasini, Frag-transitive extensions of dual affine spaces, Contrib. Algebra Geom. 40. (1999), 503–532.
- [7] N. Nakagawa, On 2-dimensional hyperovals of polar type, Utilitas Mathematica, vol 76, (2008), 101–114.
- [8] A. Pasini, Diagram Geometries, Oxford Science Publications, Clarendon Press, Oxford. (1994).
- [9] H. Taniguchi, A new family of dual hyperovals in $PG(d(d+3)/2, 2)$ with $d \geq 3$, Discrete Mathematics, 309 (2009), 418–429.
- [10] H. Taniguchi, On d -dimensional Buratti-Del Fra type dual hyperovals in $PG(3d, 2)$, preprint.
- [11] J. Thas and H. van Maldeghem, Characterizations of the finite quadric Veroneseans $\mathcal{V}_n^{2^n}$, The Quarterly Journal of Mathematics, Oxford. 55 (2004), 99–113.
- [12] S. Yoshiara, Dimensional dual hyperovals associated with quadratic APN functions, Innovations in Incidence Geometry. 8 (2009).
- [13] S. Yoshiara, Notes on split dimensional dual hyperovals, preprint, (2008).
- [14] S. Yoshiara, Ambient spaces of dimensional dual arcs, Journal of Algebraic Combinatorics. 19 (2004), 5–23.